

IN THE CLAIMS

This listing of claims replaces all prior versions:

Please cancel claims 3-8, 10-20 and 23-26

1. (**Currently Amended**) An apparatus for providing ~~verification of~~ a security status of an on-line service, comprising:

~~a database that stores a profile of devices and services comprising the on-line service and a corresponding indication of their vulnerability; and~~

~~a verification engine web page object that provides verification to visitors is automatically rendered by a browser when a visitor uses the browser to access one or more web pages of the on-line service via a public network by displaying an indication of the security status of the on-line service to the visitor in accordance with the stored profile; and~~

~~a verification service that hosts the web page object separately from the one or more web pages of the on-line service, and further controls contents of the web page object,~~

~~wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status, and~~

~~wherein the verification service causes the visual appearance contents of the indication is web page object to be automatically rendered and displayed changed in accordance with its prior determination of a level of the security status computed for the on-line service, such that when the verification service determines, in a first verification operation prior to the visitor's access request, that the on-line service has a first level of the security status, it causes the web page object to have first contents, and when the verification service determines, in a second verification operation prior to the visitor's access request, that the on-line service has a different second level of the security status, it causes the web page object to have different second contents, and thereby automatically controls the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined web page object contents when the visitor requests access to the on-line service, and~~

~~wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed by the verification~~

service prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein when the verification service causes the web page object to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser.

2. **(Currently Amended)** An apparatus according to claim 1, ~~further comprising a scanning engine that detects~~ wherein the on-line service comprises devices and services, and wherein the verification service determines the security status level of the on-line service by evaluating a vulnerability scan of the devices and services comprising the on-line service.

3-8. **(Canceled)**

9. **(Currently Amended)** An apparatus according to claim 8-2, wherein the ~~alert engine is operative to further determine whether new vulnerabilities potentially affect the on-line service based on information in the stored profile and newly received vulnerability information without requiring~~ verification service periodically receives results of a new vulnerability scan by the scanning engine to detect of the devices and services comprising the on-line service and causes the contents of the web page object to be changed if a changed security status level is determined, thereby automatically providing the visitor with an updated security status.

10-20. **(Canceled)**

21. **(Currently Amended)** A method for providing ~~verification of~~ a security status of an on-line service, comprising:

~~detecting devices and services comprising the on-line service;~~

~~comparing the detected devices and services against vulnerability fingerprints;~~

hosting a web page object separately from one or more web pages of the on-line service;

providing a link to the web page object so that it is automatically rendered by a browser when a visitor uses the browser to access the one or more web pages receiving requests for verification from visitors of the on-line service via a public network;

providing an indication of the security status of the on-line service to the visitor in accordance with a result of the comparing step via the automatic rendering of the web page object by the visitor's browser, wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status; and

changing the visual appearance contents of the indication web page object to be automatically rendered and displayed changed in accordance with a determination of a level of the security status computed for the on-line service, including:

in a first verification operation prior to the visitor's access request, causing the web page object to have first contents if the on-line service has a first level of the security status, and

in a second verification operation prior to the visitor's access request, causing the web page object to have different second contents if the on-line service has a different second level of the security status,

thereby automatically controlling the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined web page object contents when the visitor requests access to the on-line service,
wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and
wherein, when the web page object is caused to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser.

22. **(Currently Amended)** A method according to claim 21, wherein at least one of the comparing step first and second verification operations includes scanning the on-line service from a remote address on the network.

23-26. (Canceled)

27. (New) A method according to claim 21, wherein the on-line service comprises devices and services, and wherein the first and second verification operations include determining the security status level of the on-line service by evaluating a vulnerability scan of the devices and services comprising the on-line service.

28. (New) A method according to claim 27, further comprising periodically receiving results of a new vulnerability scan of the devices and services comprising the on-line service and causing the contents of the web page object to be changed if a changed security status level is determined, thereby automatically providing the visitor with an updated security status.

29. (New) A method according to claim 21, wherein the web page object comprises an image and an associated URL.

30. (New) A method according to claim 21, wherein the web page object comprises a graphical file whose contents are periodically updated in accordance with a periodically determined security status level.